**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1-8 (Canceled)

9. (Previously presented) A computer-implemented method for ensuring non-repudiation of a payment request~~, the payment request being generated in a computing environment having a connection to a network~~, the method comprising ~~the steps of~~:

receiving, at one or more computer systems operated by an organization ~~over the network~~, [[the]] a payment request identifying at least at least one payee;

receiving ~~together with~~, at the one or more computer systems operated by an organization, a certificate ~~identifying a user having caused the payment request to be generated, the certificate~~ including certificate-identifying information, [[and]] user-identifying information identifying a user having caused the payment request to be generated, ~~the certificate further including~~ and authority information defining:

an authority of the user identified in the user-identifying information to make [[the]] payment requests,

~~the authority information including~~ a maximum payment that the user identified in the user-identifying information is authorized to make, and

~~an identification of~~ a list of specific payees to whom the user identified in the user-identifying information is authorized to make payments;

~~validating the certificate identifying information and the user identifying information included within the received certificate;~~

~~accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate;~~

retrieving, with one or more processors associated with the one or more computer systems operated by an organization, ~~from the accessed store of authority information,~~ stored

authority information ~~that is~~ associated with the user identified in the user-identifying information from a store of authority information hosted outside the organization and that is independent of the received certificate;

~~comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate;~~

validating, with the one or more processors associated with the one or more computer systems operated by an organization, the authority information within the received certificate ~~only if the~~ based on a comparison between the retrieved authority information ~~matches~~ and the authority information included within the received certificate[[,]]; and

~~executing of~~ generating information, with the one or more processors associated with the one or more computer systems operated by an organization, authorizing the payment request ~~only when the certificate-identifying information, the user-identifying information and~~ in response to a validation of the authority information included within the received certificate when the at least one payee identified in the payment request is included in the list of specific payee defined in the authority information included within the received certificate ~~is successfully validated~~.

10. (Currently amended) The method of claim 9, wherein the payment request is for a predetermined amount and wherein authorizing the payment request further comprises ~~is authorized only when the validating steps are successful and when the authority information for the user stored in the hierarchical authority data structure lists an authorized amount for the user~~ authorizing the payment request when the maximum payment that the user identified in the user-identifying information is authorized to make is at least greater than or equal to the predetermined amount.

11. (Currently amended) The method of claim 9, wherein the received certificate ~~received in the receiving step~~ conforms to the X.509 standard.

12. (Currently amended) The method of claim 9, wherein the authority information included in the received certificate is configured as XML code.

13. (Original) The method of claim 9, wherein the XML code is compliant with a DSML standard.

14. (Canceled)

15. (Currently amended) A non-transitory computer-readable storage medium ~~configured to store~~ storing computer-executable code for ~~one or more software application configured to~~ carrying out a financial transaction~~, the application being configured to run on a computer coupled to a network~~, the computer-readable storage medium comprising:

certificate receiving code ~~which is~~ configured to receive a digital certificate ~~from a user over the network, the certificate~~ including certificate-identifying information, [[and]] user-identifying information identifying a user responsible for the financial transaction, ~~the certificate further including~~ and authority information ~~that defines~~ defining:

an authority ~~granted to~~ of the user to request that the financial transaction be carried out,

~~the authority information including~~ a maximum transaction amount ~~payment~~ that the user identified in the user-identifying information is authorized to make, and

~~an identification payees to~~ a list of specific parties with whom the user identified in the user-identifying information is authorized to carry out transactions ~~make payments~~;

~~certificate validating code configured to enable validation of the certificate-identifying information and user-identifying information within the received certificate, and~~

authorization validating code configured to ~~cause the computer to carry out steps of: accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate;~~ retrieving~~, from the accessed data structure,~~ stored authority information ~~that is~~ associated with the user identified in

the user-identifying information from a store of authority information stored apart from the payment request and that is independent of the received digital certificate and ~~; comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate;~~ validate[[ing]] the authority information within the received digital certificate ~~only if the~~ based on a comparison between the retrieved authority information ~~matches~~ and the authority information included within the received digital certificate[[,]]; and

code for generating information authorizing ~~executing of~~ the financial transaction ~~only when~~ in response to a validation of the authority information included within the received digital certificate when at least one party to the transaction is included in the list of specific parties defined in the authority information included within the received digital certificate ~~is successfully validated~~.

16. (Previously presented) The computer-readable storage medium of claim 15, wherein the digital certificate conforms to the X.509 standard.

17. (Currently amended) The computer-readable storage medium of claim 15, wherein the authority information included in the received digital certificate is configured as XML code.

18. (Previously presented) The computer-readable storage medium of claim 17, wherein the XML code is compliant with a DSML standard.

19. (Currently amended) The computer-readable storage medium of claim 15, wherein the authority defined [[by]] in the authority information within the received digital certificate also defines rights of the user to access predetermined data and programs associated with the financial transaction ~~within the network~~.

20-28 (Canceled)

29. (Currently amended) A server computer to authenticate a user of a client computer and to verify that the user is authorized to request that the server computer carry out a requested action, the server computer comprising:

a processor; and

a memory coupled to the processor and configured to store a set of instructions that when executed by the processor causes the processor to:

receive a payment request along with a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion,

wherein the first code portion of the digital certificate is configured to enable authentication of the user, the first code portion defining[[es]] a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field,

wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate defining access rights of the user including a maximum payment that the user is authorized to make and ~~an identification of~~ a list of specific payees to whom the user is authorized to make payments;

~~access a store of authority information that is coupled to the network, that is stored independent of the received digital certificate;~~

retrieve, from ~~the accessed~~ a store of authority information, stored authority information ~~that is~~ associated with the user of the client computer that is stored apart from the payment request and that is independent of the received digital certificate;

~~compare the retrieved authority information with the authority information included within the digital certificate to determine whether the retrieved authority information matches the authority information included within the digital certificate;~~

validate the authority information within the digital certificate ~~only if the~~ based on a comparison between the retrieved authority information ~~matches~~ and the authority information included within the digital certificate[[,]]; and

generate information authorizing the payment request ~~carry out the requested action only when~~ in response to a validation of the authority information within the digital certificate when the at least one payee identified in the payment request is included in the list of specific payee defined in the authority information included within the received certificate ~~is successfully validated~~.

30. (Previously presented) The server computer of claim 29, wherein the digital certificate conforms to the X.509 standard.

31. (Previously presented) The server computer of claim 2.9, wherein the second code portion is configured as XML code.

32. (Previously presented) The server computer of claim 31, wherein the XML code is compliant with a DSML standard.

33. (Previously presented) The server computer of claim 29, wherein the authority of the user of the client computer is stored in a hierarchical authority data structure that is accessible by the server computer.